

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

In the Matter of the Search of

IN THE MATTER OF THE SEARCH OF INFORMATION) 4:20 MJ 1322 JMB
ASSOCIATED WITH INSTAGRAM ACCOUNTS: ONLY.BRAATT) **FILED UNDER SEAL**
AND PUREEXCELLENT THAT ARE STORED AT PREMISES) SIGNED AND SUBMITTED TO THE COURT FOR
CONTROLLED BY FACEBOOK, INC.) FILING BY RELIABLE ELECTRONIC MEANS
)
)

APPLICATION FOR A SEARCH WARRANT

I, DANIEL ROOT, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

See Attachment A

located in the Northern District of California, there is now concealed

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ XX evidence of a crime;
- ☒ XX contraband, fruits of crime, or other items illegally possessed;
- ☒ XX property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

Title Section

18 U.S.C. § 2421 (Transportation with the intent to engage in criminal sexual activity)

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

Daniel P. Root 12/11/2020

Applicant's signature

Daniel Root, SA, FBI

Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41.

Date: 12-11-2020

[Signature]
Judge's signature

City and State: St. Louis, MO

Honorable John M. Bodenhause, U.S. Magistrate Judge

Printed name and title

AUSA: Jillian Anderson

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF)	
INFORMATION ASSOCIATED WITH)	No. 4:20 MJ 1322 JMB
INSTAGRAM ACCOUNTS:)	
ONLY.BRAATT AND PUREEXCELLENT)	
THAT ARE STORED AT PREMISES)	FILED UNDER SEAL
CONTROLLED BY FACEBOOK, INC.)	

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Daniel Root, a Special Agent with the Federal Bureau of Investigation, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant pursuant to 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Federal Criminal Procedure 41 for information associated with Instagram accounts “Only.braatt” and “pureexcellent” (the “Subject Accounts”) that is stored at premises owned, maintained, controlled, or operated by a social-networking company owned by Facebook, Inc. and headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. The requested warrant would require Instagram to disclose to the United States records and other information in its possession, including the contents of communications, pertaining to the subscriber or customer associated with the subject account as further described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (hereinafter referred to as “FBI”), assigned to the Violent Crimes Against Children Task Force. I have been a Special Agent of the FBI since 2016. I have conducted numerous investigations regarding the sexual exploitation of children that involve the use of a computer which has been used to commit

a crime in violation of Title 18, United States Code, Sections 2251 and 2252 (sexual exploitation of a child), Title 18, United States Code, Section 2252A (child pornography) and Title 18, United States Code, Section 2421 (transportation with intent to engage in criminal sexual activity). As an FBI Special Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have been personally involved in the execution of search warrants to search residences and seize material relating to the sexual exploitation of minors including computers, computer equipment, software, and electronically stored information. I have experience utilizing computers during my career as an investigator and I have completed multiple in-service trainings, outside trainings, and other courses in computer crime investigation. I have attended SANS external computer training and obtained the GIAC Security Essentials certificate. I have attended FBI training and been certified as a Digital Extraction Technician, allowing me to image, search, find, and extract evidence from digital devices.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. §2421 have been committed by Markezz Manuel. There is also probable cause to search the information described in Attachment A for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

LOCATION TO BE SEARCHED

5. The location to be searched is:

Information associated with the Instagram profile and account with usernames: “Only.braatt” and “pureexcellent” (hereinafter referred to as “Subject Accounts”) stored and located at premises owned, maintained, controlled, or operated by a social-networking company owned by Facebook, Inc. and headquartered in Menlo Park, California, at 1601 Willow Road, Menlo Park, California 94025, further described in Attachment A. The items to be reviewed and seized by the United States are described in Attachment Part II of Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

BACKGROUND RELATING TO INSTAGRAM

7. The Internet is in part a computer communications network using interstate and foreign telephone and communication lines to transmit data streams, including data streams used to provide a means of communication from one computer to another and used to store, transfer and receive data and image files.

8. An “Internet Protocol” (IP) address is a unique series of numbers, separated by a period, that identifies each computer using, or connected to, the Internet over a network. An IP address permits a computer (or other digital device) to communicate with other devices via the Internet. The IP addresses aids in identifying the location of digital devices that are connected to the Internet so that they can be differentiated from other devices. As a mailing address allows a

sender to mail a letter, a remote computer uses an IP address to communicate with other computers.

9. An “Internet Service Provider” (ISP) is an entity that provides access to the Internet to its subscribers.

10. The term “remote computing service” means the provision to the public of computer storage or processing services by means of an electronic communications system.

11. Instagram, LLC is a business and company that operates as a remote computing service, a provider of electronic communications services through ISPs.

12. From my review of publicly available information provided by Instagram about its service, including Instagram’s “Privacy Policy,” I am aware of the following about Instagram and about the information collected and retained by Instagram.

13. Instagram operates a free-access social-networking website of the same name that can be accessed at <http://www.instagram.com>. Instagram allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and other information. Users can access Instagram through the Instagram website or by using a special electronic application (“app”) created by the company that allows users to access the service through a mobile device.

14. Instagram permits users to post photos to their profiles on Instagram and otherwise share photos with others on Instagram, as well as certain other social-media services, including Flickr, Facebook, and Twitter. When posting or sharing a photo on Instagram, a user can add to the photo: a caption; various “tags” that can be used to search for the photo (e.g., a user made add the tag #vw so that people interested in Volkswagen vehicles can search for and find the photo); location information; and other information. A user can also apply a variety of

“filters” or other visual effects that modify the look of the posted photos. In addition, Instagram allows users to make comments on posted photos, including photos that the user posts or photos posted by other users of Instagram. Users can also “like” photos.

15. Upon creating an Instagram account, an Instagram user must create a unique Instagram username and an account password. This information is collected and maintained by Instagram.

16. Instagram asks users to provide basic identity and contact information upon registration and also allows users to provide additional identity information for their user profile. This information may include the user’s full name, e-mail addresses, and phone numbers, as well as potentially other personal information provided directly by the user to Instagram. Once an account is created, users may also adjust various privacy and account settings for the account on Instagram. Instagram collects and maintains this information.

17. Instagram allows users to have “friends,” which are other individuals with whom the user can share information without making the information public. Friends on Instagram may come from either contact lists maintained by the user, other third-party social media websites and information, or searches conducted by the user on Instagram profiles. Instagram collects and maintains this information.

18. Instagram also allows users to “follow” another user, which means that they receive updates about posts made by the other user. Users may also “unfollow” users, that is, stop following them or block the, which prevents the blocked user from following that user.

19. Instagram allow users to post and share various types of user content, including photos, videos, captions, comments, and other materials. Instagram collects and maintains user content that users post to Instagram or share through Instagram.

20. Instagram users may send photos and videos to select individuals or groups via Instagram Direct. Information sent via Instagram Direct does not appear in a user's feed, search history, or profile.

21. Users on Instagram may also search Instagram for other users or particular types of photos or other content.

22. For each user, Instagram also collects and retains information, called "log file" information, every time a user requests access to Instagram, whether through a web page or through an app. Among the log file information that Instagram's servers automatically record is the particular web requests, any Internet Protocol ("IP") address associated with the request, type of browser used, any referring/exit web pages and associated URLs, pages viewed, dates and times of access, and other information.

23. Instagram also collects and maintains "cookies," which are small text files containing a string of numbers that are placed on a user's computer or mobile device and that allows Instagram to collect information about how a user uses Instagram. For example, Instagram uses cookies to help users navigate between pages efficiently, to remember preferences, and to ensure advertisements are relevant to a user's interests.

24. Instagram also collects information on the particular devices used to access Instagram. In particular, Instagram may record "device identifiers," which includes data files and other information that may identify the particular electronic device that was used to access Instagram.

25. Instagram also collects other data associated with user content. For example, Instagram collects any "hashtags" associated with user content (i.e., keywords used), "geotags"

that mark the location of a photo and which may include latitude and longitude information, comments on photos, and other information.

26. Instagram also may communicate with the user, by email or otherwise. Instagram collects and maintains copies of communications between Instagram and the user.

27. As explained herein, information stored in connection with an Instagram account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, an Instagram user’s account activity, IP log, stored electronic communications, and other data retained by Instagram, can indicate who has used or controlled the Instagram account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the Instagram account at a relevant time. Further, Instagram account activity can show how and when the account was accessed or used. For example, as described herein, Instagram logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Instagram access, use, and events relating to the crime under investigation. Additionally, Instagram builds geo-location into some of its services. Geo-location allows, for example, users to “tag” their location in posts and Instagram “friends” to

locate each other. This geographic and timeline information may tend to either inculcate or exculpate the Instagram account owner. Last, Instagram account activity may provide relevant insight into the Instagram account owner's state of mind as it relates to the offense under investigation. For example, information on the Instagram account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

28. Based on the information above, the computers of Instagram are likely to contain all the material described above with respect to the SUBJECT ACCOUNT, including stored electronic communications and information concerning subscribers and their use of Instagram, such as account access information, which would include information such as the IP addresses and devices used to access the account, as well as other account information that might be used to identify the actual user or users of the account at particular times.

PROBABLE CAUSE

29. The following terms have the indicated meaning in this Affidavit:

- a. The term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such a device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device. 18 USC § 1030(e).
- b. The term "minor" means any individual under the age of 18 years. 18 USC § 2256(1).

- c. “Sexually explicit conduct” means actual or simulated sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person. 18 USC § 2256(2).
- d. Visual depiction includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image. 18 USC § 2256(5).
- e. “Child pornography” means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. 18 USC 2256 § (8)(A) and (C).
- f. “Identifiable minor” means a person who was a minor at the time the visual depiction was created, adapted, or modified; or whose image as a minor was used in creating, adapting, or modifying the visual depiction; and who is recognizable as an actual person by the person’s face, likeness, or other distinguishing characteristic, such as a unique birthmark or other recognizable feature; and shall not be construed to require proof of the actual identity of the identifiable minor. 18 USC § 2256(9).
- g. The Internet is in part a computer communications network using interstate and

foreign telephone lines to transmit data streams, including data streams used to provide a means of communication from one computer to another and used to store, transfer and receive graphic image files.

30. On 30 November 2020, your Affiant responded to a report of a missing 14-year old juvenile who was suspected to be in the company of 30-year old Markezz Manuel en route to Florida without parental permission.

31. According to the missing juvenile's mother, the juvenile (hereinafter referred to as Z.I.) had written a note that she was going to stay with family, and had left her house.

32. Z.I.'s mother believed her to be in the company of Markezz Manuel.

33. Manuel was previously a roommate of Z.I.'s maternal grandmother.

34. In or around July of 2020, Z.I. and her mother moved across the street from Z.I.'s maternal grandmother and Z.I. began to have more interaction with Manuel.

35. It was reported to detectives that Manuel had previous accusations of improper relationships with minors, though no convictions. A search of his criminal history indicated a sexual assault charge that was not prosecuted.

36. Once Z.I. was reported missing, call records, serving cell site information, and geolocation data was requested for the cell phone number used by Markezz Manuel, (314) 405-1452.

37. Your Affiant reviewed the call detail records (CDR) with associated tower data for target number (314) 405-1452.

38. At 11/28/2020 23:57:18 UTC, the handset was serviced by a T-Mobile tower located at 38.709387, -90.335785. This tower is within 2500 meters of Z.I.'s residence.

39. At 11/29/2020 19:14:38 UTC, the handset was serviced by a T-Mobile tower

located at 33.053179, -83.948335. This tower is located in Forsyth, Georgia.

40. At 11/30/2020 21:02:25 UTC, the handset was serviced by a T-Mobile tower located at 28.565581, -81.287696. This tower is located in Orlando, Florida.

41. Once Z.I. was reported missing, a canvass of her friends resulted in the identification of a friend, V.J., who reported speaking with Z.I. on Instagram recently.

42. V.J. stated that Z.I. referred to Manuel as her “boyfriend” and stated that they were stuck in traffic in Atlanta the last time they talked.

43. The communication took place via Instagram video chat. Z.I. contacted her from Instagram account “Only.braatt.”

44. Your Affiant responded to the workplace of V.J.’s mother and retrieved V.J.’s cell phone.

45. After a forensic extraction of the cell phone, your Affiant located remnants of the Instagram text chats between V.J. and Z.I. They were incomplete due to the user of the phone attempting to delete them prior to the extraction.

46. At 11/30/2020 02:09:30 CST, Z.I. said to V.J. via Instagram using the account Only.braatt, “And yk what to say it she call yu haven't spoke to me nene !”

47. A request was sent to Instagram to provide login information for the account Only.braatt. Instagram responded that the most recent login was from IPv6 address 22607:fb90:42f3:887a:55a9:577a:4424:d84f at 2020-11-30T17:28 UTC.

48. A request was sent to T-Mobile to identify the handset that was assigned that IPv6 address. T-Mobile responded with the subscriber number (314) 405-1452.

49. Through this, your Affiant determined it was likely that Z.I. did not have her own phone and was using Manuel’s phone to log into her Instagram.

50. The location data from the handset using (314) 405-1452 was provided to the Orange County, Florida Sheriff's Office.

51. Deputies located and detained Markezz Manuel in Orlando, Florida. He initially told deputies that he had left Z.I. in St. Louis, Missouri.

52. After further questioning, he admitted that this was not the case and led deputies to a stairwell in an apartment complex where he had told her to hide should they become separated.

53. Z.I. was taken into police custody until her mother arrived on a flight to bring her back to St. Louis.

54. On 1 December 2020, Z.I. and her mother landed in St. Louis.

55. Your Affiant met with Z.I. and interviewed her about the events surrounding her trip to Florida.

56. Z.I. stated that Manuel referred to her as his girlfriend and that they had been engaged in a sexual relationship since around July 2020.

57. Z.I. stated that Manuel would typically communicate with her via Instagram using his account, "pureexcellent." The communication was almost exclusively on Instagram as she did not even know his phone number.

58. A review of the account pureexcellent shows photographs of Manuel.

59. Z.I. stated that they would talk about the sexual nature of their relationship in the Instagram chats.

60. Z.I. and her mother consented to a search of the chats, but the password had been changed since she had logged in using Manuel's phone.

61. Due to the potential for either party to delete the chats, your Affiant served a

preservation order on Instagram for both accounts listed in this affidavit.

62. On 2 December 2020, Manuel called the FBI Orlando office to request his phone back.

63. Your Affiant believes that the content of the messages sought in this warrant will demonstrate the intent of Manuel in transporting Z.I. across state lines, and will consist of evidence of violations of 18 USC § 2421.

64. Based on the above information, there is probable cause to believe that the items listed in Attachment A constitute evidence of violations of Title 18, United States Code, Section 2421, among others, and will be found in the electronic or wire communications stored by Instagram.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

65. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

66. Based on the forgoing, I request that the Court issue the proposed search warrant. The United States will execute this warrant by serving the warrant on Instagram. Because the warrant will be served on Instagram, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

67. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

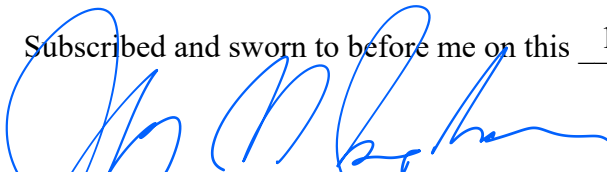
68. I further request that the Court order that all papers in support of this application, including the affidavit and warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

 12/11/2020

Daniel Root
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on this 11th day of December, 2020


The Honorable John M. Bodenhause
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Instagram profile and account with usernames “Only.braatt” and “pureexcellent” stored and located at premises owned, maintained, controlled, or operated by FACEBOOK, INC., a social-networking company owned headquartered in Menlo Park, California, at 1601 Willow Road, Menlo Park, California 94025.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Instagram, LLC

To the extent that the information described in Attachment A is within the possession, custody, or control of Instagram, LLC, including any messages, records, files, logs, or information that have been deleted but are still available to Instagram, LLC, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Instagram, LLC is required to disclose the following information, from July 1, 2020 to December 10, 2020, to the government for each account listed in Attachment A:

- a. All identity and contact information, including full name, e-mail address, physical address (including city, state, and zip code), date of birth, phone numbers, gender, hometown, occupation, and other personal identifiers;
- b. All past and current usernames associated with the account;
- c. The dates and times at which the account and profile were created, and the Internet Protocol (“IP”) address at the time of sign-up;
- d. All activity logs including IP logs and other documents showing the IP address, date, and time of each login to the account, as well as any other log file information;
- e. All information regarding the particular device or devices used to login to or access the account, including all device identifier information or cookie information, including all information about the particular device or devices used to access the account and the date and time of those accesses;
- f. All data and information associated with the profile page, including photographs, “bios,” and profile backgrounds and themes;
- g. All communications or other messages sent or received by the account;
- h. All user content created, uploaded, or shared by the account, including any comments made by the account on photographs or other;
- i. All photographs and images in the user gallery for the account;
- j. All location data associated with the account, including geotags;
- k. All data and information that has been deleted by the user;

- l. A list of all of the people that the user follows on Instagram and all people who are following the user (*i.e.*, the user's "following" list and "followers" list), as well as any friends of the user;
- m. A list of all users that the account has "unfollowed" or blocked;
- n. All privacy and account settings;
- o. All records of searches performed by the account, including all past searches saved by the account;
- p. All information about connections between the account and third-party websites and applications; and,
- q. All records pertaining to communications between Instagram, LLC and any person regarding the user or the user's Instagram account, including contacts with support services, and all records of actions taken, including suspensions of the account.

Instagram, LLC is hereby ordered to disclose the above information to the United States within 14 days of the date of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of federal involving the exploitation of minors including violations of 18 U.S.C. §§1470, 2422, 2251, 2252A, 2422 or 2423, involving Markezz Manuel from July 1, 2020 to December 10, 2020, including, for each username identified on Attachment A, information pertaining to the following matters:

- (a) All data, material and information related to or involving a juvenile known to law enforcement whose initials are Z.I. or other data, material and information of asexual nature related to minors;
- (b) Evidence indicating how and when the Instagram account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the Instagram account owner;

- (c) Evidence indicating the Instagram account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s);
- (e) The identity of person(s) who communicated with the user ID about matters involving a juvenile whose initials are Z.I. and about matters of a sexual nature involving minors, including records that help reveal their whereabouts;
- (f) All activity logs for the account and all other documents showing the user's posts and other Instagram activities from July 1, 2020 to December 10, 2020;
- (g) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in them July 1, 2020 to December 10, 2020, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;
- (h) All profile information; All posts including videos, photographs, articles, and other items; comments; tags; and information about the user's access and use of Instagram applications between July 1, 2020 and December 10, 2020;
- (i) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;
- (j) All other records and contents of communications and messages made or received by the user from July 1, 2020 to December 10, 2020, including all Direct Message (DM) activity and video chat;

- (k) All applications and related materials used to apply for an Instagram “verified badge;”
- (l) All “check ins” and other location information between July 1, 2020 and December 10, 2020;
- (m) All IP logs, including all records of the IP addresses that logged into the account between July 1, 2020 and December 10, 2020;
- (n) All records of the account’s usage of the “Like” feature, including all Instagram posts and all non-Instagram webpages and content that the user has “liked” between July 1, 2020 and December 10, 2020;
- (o) All information about the Instagram pages that the account “follows” between July 1, 2020 and December 10, 2020;
- (p) All connected social media accounts including, but not limited to Snapchat, Twitter, Facebook, Foursquare, Tumblr, Flickr, and VK between July 1, 2020 and December 10, 2020;
- (q) All lists of “follows” created by the account between July 1, 2020 and December 10, 2020;
- (r) All records of Instagram searches performed by the account from July 1, 2020 to December 10, 2020
- (s) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number); and
- (t) All privacy settings and other account settings, including privacy settings for individual Instagram posts and activities, and all records showing which Instagram users have been blocked by the account.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Instagram, LLC, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Instagram, LLC. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Instagram, LLC, and they were made by Instagram, LLC as a regular practice; and

b. such records were generated by Instagram, LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Instagram, LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Instagram, LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature